METHOD AND APPARATUS FOR ENCODING SECURITY STATUS INFORMATION

This application is a non-provisional application claiming priority from United States Provisional Application No. 60/431,078 and United States Provisional Application No. 60/431,645.

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0001] The present invention relates to a method and apparatus for encoding security status information.

DESCRIPTION OF THE PRIOR ART

[0002] Low rate personal wireless networks are used with small devices with transmission speeds of up to 250 kilobits per second. These devices typically have severe power constraints as they are operated on batteries. In many of these devices, such as battery-operated sensors, remote controls, car door openers and light switches, it is necessary to have long battery life. If the batteries die too quickly then the replacement cost can be equal to the cost of the product itself.

[0003] It is also desirable to have secure communications between such constrained devices to prevent abuse of the system. One technique is to encrypt data being sent between the devices. Encryption mathematically transforms the transmitted information using a secret key known only to the two parties who are communicating. Without the key, the message is unintelligible. However, this requires overhead in the message structure in order to allow the recipient to decrypt the data. The sender must indicate which key it has used, which algorithm it has used to encrypt, and input parameters of the encryption algorithm such as a counter.

[0004] Usually, a frame counter is used as one of the input parameters for freshness in the encryption. Freshness means that the parameters change for each communication and are thus not reused. One type of encryption called a block cipher breaks up a message into parts (blocks)

of a fixed size. Various block ciphers are known such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard). Block ciphers often use an input block as a seed when used in stream-cipher mode. This input block should not repeat in order to maintain data freshness and data confidentiality. In one approach, a frame counter and a key identifier are used as the input block and are indicated in the message that is sent. In addition, each message usually includes a sequence counter that is not used for security but rather to match the sending of a message with the acknowledgement thereof by the recipient. These messages typically include a data portion referred to as the payload which is about 20 bytes. Accordingly, a five byte overhead for security information represents a 25% overhead.

[0005] The amount of data transferred between such constrained devices is one of the principal factors in their battery life. Accordingly, it is desirable to reduce the amount of information transferred.

[0006] However, in order to maintain the security of the underlying encryption methods, the number of bits in the frame counter should not be reduced.

SUMMARY OF THE INVENTION

[0007] In accordance with one aspect of the present invention there is provided a method of encoding a frame counter used in communication between a sender and a receiver. The method comprises maintaining a sequence counter and a frame counter at the sender and computing new values of the frame counter such that the frame counter is unique and recoverable from an encoded value of the frame counter and the sequence counter.

[0008] In another aspect there is provided a method of transmitting messages from a sender to a recipient over a wireless channel, the messages including a sequence counter and a frame counter. The method comprises establishing initial values of the sequence counter and the frame counter at the sender. Initial values of the frame counter and the sequence counter are provided to the recipient. The sender sends compressed messages including the value of the sequence counter and not the frame counter and monitors for an acknowledgement of receipt by the recipient. When no acknowledgment is received, the sender sends uncompressed messages until an acknowledgement of receipt is received from the recipient. The sequence counter is

incremented and the next value of the frame counter is established as the integer next larger than previous value of the frame counter which is congruent to the sequence counter modulo 256.

[0009] In yet another aspect, there is provided a method of transmitting messages from a sender to a recipient over a wireless channel, the messages including a sequence counter and a frame counter. The method comprises establishing initial values of the sequence counter and the frame counter at the sender and providing the initial values of the frame counter and the sequence counter to the recipient. The sender sends compressed messages including the value of the sequence counter and not the frame counter. Periodically the sender sends uncompressed messages including the value of the frame counter according to predefined criteria. The sender increments the sequence counter and establishes the next value of the frame counter as the integer next larger than previous value of the frame counter which is congruent to the sequence counter modulo 256.

[0010] In a further aspect, there is provided a wireless device for receiving communications from other wireless devices in a wireless network. The device comprises storage for a frame counter, a receiver for obtaining a message over the wireless network, the message including a sequence counter and data encrypted using a secret key and a new value of the frame counter as input to the encryption. The device includes a decryptor configured to perform decryption complementary to the encryption used in the message, the decryptor having access to the secret key. A processor is connected to the message receiver and configured to recover the value of the frame counter from a sequence counter in the message and provide the frame counter and encrypted data from the message to the decryptor.

[0011] In a yet further aspect, there is provided a wireless device for sending communications to other wireless devices in a wireless network. The device comprises storage for a frame counter and a sequence counter and a processor to compute a new value of the frame counter such that the frame counter is unique and recoverable from an encoded value of the frame counter and the sequence counter. The device further includes a transmitter for sending a message over the wireless network, the message including a sequence counter and data encrypted using a secret key and the new value of the frame counter as input to the encryption.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] These and other features of the preferred embodiments of the invention will become more apparent in the following detailed description in which reference is made to the appended drawings wherein:

[0013] Figure 1 is a schematic representation of a communication system.

[0014] Figure 2 is a more detailed view of a correspondent in the communication system of Figure 1.

[0015] Figure 3 is a schematic representation of a message packet used by the correspondents of Figure 1.

[0016] Figure 4 is a schematic representation of another embodiment of a message packet.

[0017] Figure 5 is a schematic representation of an information exchange by the correspondents of Figure 1.

[0018] Figure 6 is a schematic representation of an information interchange among the coresponderits of Figure 1.

[0019] Figure 7 is a schematic representation of the method used in Figure 6.

[0020] Figure 8 is a schematic representation of an information exchange between the correspondents of Figure 1.

[0021] Figure 9 is a schematic representation of the method used in Figure 8.

[0022] Figure 10 is a schematic representation of the method used in Figure 9.

[0023] Figure 11 is a schematic representation of another information exchange between the correspondents of Figure 1.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0024] As may be seen in Figures 1 and 2, a communication system 10 consists of correspondents 12, 14, 16, and 18 communicating over a wireless network 20. Correspondent 12 includes a processor 22, a storage medium 24, a frame counter 26, a user interface 28. The processor 22 and storage 24 may be provided in an integrated circuit. The frame counter 26 is

used as input to an encryption method in the processor 22. The user interface 28 may be provided by a simple switch and an LED or by more sophisticated means such as a keyboard and a monitor or other display. Each correspondent includes a wireless network interface 29 which sends and receives signals at a predetermined radio frequency such as 2.4GHz or 868 MHz/915 MHz. The correspondents can communicate directly with each other when they are in close enough proximity. The network 20 also provides wireless interfaces linked to routers, bridges, and other network hardware to provide connectivity beyond the range of wireless signals and to assist in establishing connections between physically close correspondents.

[0025] The correspondents exchange messages using packets in the format shown in Figure 3 by the numeral 30. The packet consists of three portions: a header 32, a payload 40, and a footer 48. The header 32 contains a frame control portion 34, a sequence counter 36 which is notated as DSN and addressing fields 38. The payload portion 40 contains the actual content of the message, and includes security status information and data 46. The security status information 42, 44 includes a compressed frame counter 42 and a key identifier 44. The footer portion 48 of the packet 30 includes an error control sequence. As shown in Figure 2, the compressed frame counter 42 and the sequence counter 36 together form the frame counter 50.

[0026] In operation, the header is used to direct the packet to its intended address using the addressing fields. At the recipient, the footer is used to perform error correction and to ensure that the message has been received intact. In addition, the recipient may acknowledge the message. The acknowledgement will include the sequence counter DSN. The sequence counter is used to match sent messages with their acknowledgements. The security status information includes a frame counter which is used as input to a decryption method at the recipient. The decryption method is then used to decode the data and recover the original data sent by the sender.

[0027] In order to reduce the amount of information transferred, the frame counter is specially encoded. This encoding is accomplished by updating the frame counter N to a value of $N_0 \geq N$ such that $N_0 = \min\{N' \geq N \text{ such that } N' = DSN \bmod 256\}$. The frame counter can then be represented as 3 byte encoded frame counter portion with the sequence counter DSN

appended thereto. Accordingly, it is only necessary to transmit 3 bytes in the payload portion to communicate the frame counter rather than the full length of 4 bytes.

[0028] In another embodiment, further reduction in the information transferred may be achieved by omitting the frame counter altogether from the payload as seen in Figure 4. The sequence counter DSN is then used to recover the new value of the frame counter by combining the previous value of the frame counter 42 in storage 24 with the value of the sequence counter. In this embodiment, the message is compressed by removing the frame counter entirely.

[0029] Referring therefore to Figure 5, a simplified information exchange between one sender and one recipient is shown. The sender begins with a frame counter of 270. The sender transmits the frame counter 270 to the recipient. The recipient is then initialised to the beginning value of 270. For each further communication, the sequence counter is incremented. Accordingly, the next message has a sequence counter of 15 and a frame counter of 271. The sender sends the value of the sequence counter, which is 15 and equal to 271 mod 256, to the recipient. The recipient then updates the frame counter with the integer next larger to 270 which is congruent to 15 mod 256, in this case the value 271. Each sequential communication proceeds similarly with the sequence counter being incremented. Accordingly, the next transmission of a frame counter 272 is accomplished by transmitting the sequence counter of 16. The recipient may then recover the value 272 of the frame counter from the sequence counter 16 and the previous frame counter 271.

[0030] In typical use, the sender will be communicating with several recipients and accordingly the messages may be spaced out in time. There may be intervening messages to other recipients which necessitate incrementing the sequence control DSN between messages to any given recipient. Accordingly, the consecutive structure shown in Figure 5 may not always be present. The communication may proceed as shown in Figure 6 by the numeral 70. In this case, the frame counter begins at 7, which is sent to the first recipient which sets its frame counter to 7. In this example some time passes before the next message is transmitted to the first recipient. In this case, the next message is transmitted with a frame counter of 258 indicating that 250 other messages have been transmitted to other recipients by the sender in the interim. The value 258 is transmitted by sending the sequence counter, which is 258 mod 256 = 2. The

recipient then recovers 258 as the integer next larger than 7 which is congruent to 2 mod 256. The next message is transmitted with a frame counter of 289 which is transmitted by sending the sequence counter of 33. However, in this case, the recipient does not acknowledge receipt of this message. The non-acknowledgement may occur for a number of reasons including simply not receiving the message or a failure in the error control. Accordingly, the recipient's frame counter remains at 258. Since the message is not acknowledged, the sender retransmits the full value 289 of the frame counter. This retransmission resets the frame counter at the recipient to the value 289 and the recipient acknowledges with the value 33 = 289 mod 256. The final message sent immediately following the third message is 290, which is communicated by sending the sequence counter of 34 which is 290 mod 256. The recipient updates its frame counter to 290 and acknowledges receipt of the value 34.

[0031] In the above example, the recipient always acknowledges messages from the sender. Accordingly, the sender is immediately notified that a message has not been received because it does not receive an acknowledgement. In this case, the sender can send a full message to resynchronise transmission.

[0032] Referring to Figure 7, the steps of the above method are shown generally by the numeral 80. The sender first sends a compressed message at step 82. The compressed message includes the value of the sequence counter and not the frame counter. Upon receipt of the compressed message, the recipient updates its frame counter as the minimum value larger than the current frame counter which is congruent to the sequence counter modulo 256. If the message is acknowledged at step 84 then execution continues. Otherwise, the sender repeatedly sends uncompressed messages at step 86 until one of these is acknowledged. The uncompressed messages include the frame counter. Upon receipt of the uncompressed message, the recipient updates its frame counter to the value of the frame counter in the uncompressed message. Once the message is acknowledged, the sender increments the sequence counter for the next message at step 88. It is particularly expedient to increment the sequence counter by 1, however it will be recognized that other method of updates the sequence counter may be used by the sender. The sender then establishes the frame counter for the next message as the minimum value larger then the current frame counter which is congruent to the sequence counter modulo 256.

[0033] In an alternative embodiment, the recipient does not acknowledge messages received. The sender continues to transmit regardless of whether the messages are actually received. Accordingly, it is necessary for the sender to occasionally send uncompressed messages containing the value of the frame counter in case a loss of synchronisation has occurred. Referring therefore to Figure 8, the messages transmitted by the sender are shown generally by the numeral 100. The first message reaches the recipient and accordingly both the sender and the recipient have frame counters of 7. However, the second message is lost during transmission. Accordingly, the recipient's frame counter is not updated. The third message is an uncompressed message and accordingly, updates the recipient's frame counter to 288, regardless of the earlier loss of synchronisation. The fourth message 289 is sent with the sequence counter of 33 and not the frame counter. This updates the recipient's frame counter to 289. The fifth message 547 is lost during the transmission, and accordingly the recipient's frame counter is incorrect. The next message 601 is transmitted as the sequence counter of 89, which results in an incorrect frame counter at the recipient since the computation yields the value 345 which is congruent to 89 modulo 256 but differs by 256 from the value of the frame counter in the sender. The incorrect frame counter results in a failure of decryption. Upon discovering the failure, the recipient maintains its frame counter of 289 rather than updating the frame counter to the incorrect value. The final message 805 is sent as an uncompressed message which updates the recipient's frame counter to the correct value again.

[0034] The steps performed in the example of Figure 8 are shown schematically in Figure 9 by the numeral 10. The sender first sends a compressed message at step 12. The sender then increments the sequence control at step 114 then updates the frame counter at step 116. The sender then checks to see if it is time for resynchronisation at step 118. Resynchronisation can be performed at periodic intervals such as every 2, 3, 4...., 10 transmissions. When the resync is required, the sender sends an uncompressed message at step 120, otherwise the sender proceeds to send compressed messages at step 112. It will be recognized that the sender independently decides which messages to send uncompressed. The sender cannot be guided by the recipient in this choice since there is no feedback from the recipient.

[0035] In a further embodiment, the recipient occasionally acknowledges messages. Furthermore, the sender may indicate in the header of a sent message that this message should be acknowledged. The recipient can therefore use such messages to indicate that a loss of synchronisation has occurred. Referring therefore to Figure 10, a transmission is shown by the numeral 130. The first message 7 is sent and is acknowledged by the recipient. Both the sender and the recipient have frame counters of 7. The second frame counter 258 is communicated by sending the sequence counter of 2 and is lost during transmission. The third message 288 is sent as the sequence counter of 32. The recipient acknowledges receipt of the sequence counter 32 however, during the subsequent decryption, the recipient has an error since its frame counter is out of sync with the sender since the reconstructed value is 32 rather than 288. Accordingly, the recipient enables an error flag. The next message 289 is sent as the sequence counter of 33, but is rejected by the recipient due to the error flag. Another message with a frame counter of 290 is sent to the recipient as the sequence counter of 34 and with a request for acknowledgement embedded in the message. When a recipient receives this message, it does not acknowledge since the error flag is set. Therefore, the sender resends the message with the frame counter of 290 as an uncompressed message which resynchronizes the frame counters of the sender and the recipient again. The recipient then acknowledges receipt of the message with frame counter 290. The error flag indicates that a decryption error occurred and that synchronization must be established by received an uncompressed message including the frame counter, rather than a compressed message without the frame counter. It will be recognized that loss of synchronization may occur in this embodiment, but the synchronization is re-established with a delay of at most one acknowledged message.

[0036] Referring to Figure 11, the steps of this embodiment are shown schematically by the numeral 140. The sender first sends a compressed message at step 142. The recipient then acknowledges receipt of the uncompressed message at step 144. The recipient attempts to decrypt the message at step 146. If there is a failure during decryption at step 148, then the recipient sets an error flag at step 150. If there is no failure and the error flag is set, then the recipient clears the error flag at step 152. The sender then sends another compressed message at step 154. When the recipient receives the message, it checks to see if the error flag is set at step

156. If the error flag is not set, then the recipient acknowledges the message at step 158 and proceeds with decryption by steps 146 onward. If the flag is set, then the recipient does not acknowledge the message at step 160. If the message was sent with an acknowledgement request at step 162, then the sender detects this and sends an uncompressed message at step 164, and execution returns to the decryption step 146. If no acknowledgement request was sent, then the sender proceeds to send compressed messages at step 154.

[0037] It will be recognised that in these embodiments, a reduction in the amount of data transferred is achieved. The reduction is realized by maintaining frame counters at both the sender and the recipient. The inventor has recognized that the recipient can reconstruct the correct value of the frame counter from partial information received from the sender in combination with the recipient's local copy of the information. Furthermore, a recovery mechanism is provided which re-synchronizes frame counters that end up out-of-synchronization. It will be recognized that the recovery mechanism allows the compression technique to be applied in a robust manner.

[0038] It will be recognized that the above techniques are not limited to use with integers but rather may be used with counters that are elements of a finite set with a partial ordering. Furthermore, although the technique has been described in the particularly advantageous setting of a cryptographic system, it may be applied in other settings where counters are used and where a reduction in communication cost is at a premium. One example of such a setting is the inclusion of frame counters to facilitate detection of duplicate transmission.

[0039] Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as outlined in the claims appended hereto.